

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-295800

(43)Date of publication of application : 10.11.1995

(51)Int.Cl.

G06F 9/06

H04L 9/22

(21)Application number : 06-106316

(71)Applicant : ADVANCE CO LTD

(22)Date of filing : 22.04.1994

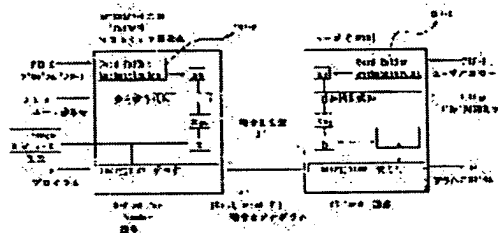
(72)Inventor : OTSUKI KAZUNORI  
WATANABE SHINICHIRO

## (54) SOFTWARE PROTECTING SYSTEM

## (57)Abstract:

PURPOSE: To enable right users to use software to be a target but to prevent the other users from using the software though they can copy the software.

CONSTITUTION: A center performs center algorithm for software and the identification data of a user and prepares secret algorithm which is exclusive for software and the user. When the supply of software is generated between a software supply body and the user, the software supply body inputs the identification data of the user in the secret algorithm of software to be a supply object, prepares the same and specific cryptographic key between the software to be the supply object and the user, ciphers the part or all the software to be the supply object by this cryptographic key and supplies the ciphered matter to the user. The user inputs the identification data of the supplied software in his own secret algorithm, prepares the same and specific cryptographic key between the supplied software and the user and decodes ciphering software.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平7-295800

(43)公開日 平成7年(1995)11月10日

(51) Int.Cl.<sup>8</sup>

G O 6 F 9/06

H04L 9/22

識別記号

5 5 0 C 7230-5B

片内整理番号

FI

### 技術表示箇所

H04L 9/04

審査請求 未請求 請求項の数1 FD (全 6 頁)

(21)出願番号

特願平6-106316

(22) 出題日

平成6年(1994)4月22日

(71)出願人 000126757

株式会社アドバンス

東京都中央区日本橋小舟町5番7号

(72)発明者 大槻 和則

神奈川県横浜市旭区中希望が丘35-2

(72)発明者 渡辺 晋一郎

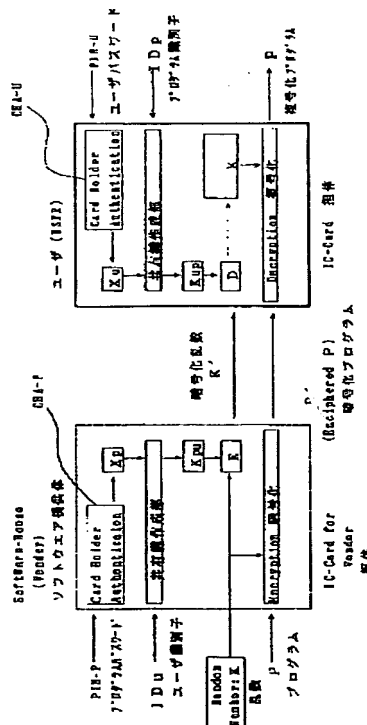
東京都江戸川区小松川 1-2-3 コーシ  
ヤタワー小松川902

(54) 【発明の名称】 ソフトウェアプロテクト方式

(57) 【要約】 (修正有)

【目的】ターゲットとなるソフトウェアを、正当なユーザは、使用できるが、その他のユーザは、コピーはできても使用できないようにする。

【構成】センタは、ソフトウェア並びにユーザの識別子にセンタアルゴリズムを施して各ソフトウェア並びにユーザに専用の秘密アルゴリズムを作成し、ソフトウェア供給体とユーザとの間で、ソフトウェアの供給が生じた場合、ソフトウェア供給体は、ユーザの識別子を供給対象となるソフトウェアの秘密アルゴリズムに入力して、供給対象となるソフトウェアとユーザとの間で同一且つ固有の暗号鍵を作成し、この暗号鍵で供給対象となるソフトウェアの一部又は全部を暗号化してユーザへ供給し、ユーザは、供給されたソフトウェアの識別子を自己の秘密アルゴリズムに入力して、供給されたソフトウェアとユーザとの間で同一且つ固有の暗号鍵を作成し暗号化ソフトウェアを復号化する。



## 【特許請求の範囲】

【請求項1】 センタが特別なアルゴリズム、すなわちセンタだけが秘密に保持するセンタアルゴリズムを作成し、センタは、ソフトウェア並びにユーザのそれぞれに用いられる各ソフトウェア並びにユーザの識別子にセンタアルゴリズムを施して各ソフトウェア並びにユーザに専用の秘密アルゴリズムを作成し、ユーザ及びソフトウェアに供給するという準備を行った後、ソフトウェアの供給体は、ユーザの識別子と供給対象となるソフトウェアの秘密アルゴリズムとにより、供給対象となるソフトウェアとユーザとの間で同一の暗号鍵を作成し、この暗号鍵に基づいて直接的又は間接的に供給対象となるソフトウェアの一部又は全部を暗号化してユーザへ供給し、ユーザは、供給されたソフトウェアの識別子と自己の秘密アルゴリズムとにより供給されたソフトウェアとユーザとの間で同一の暗号鍵を作成し暗号化ソフトウェアを直接的又は間接的に復号化することを特徴とするソフトウェアプロテクト方式。

## 【発明の詳細な説明】

## 【0001】

【利用分野】 本発明はアプリケーションソフトウェア、OS、等のソフトウェアをプロテクトする方式に関する。

## 【0002】

【従来技術】 現在、アプリケーションプログラム、OS用ソフトウェア、ユーティリティプログラム等の無断コピーは、日常的であってしかも無断コピーによる不正使用にたいする防御について充分なものは、未だ提案されるに到っていない。

## 【0003】

【課題を解決する手段】 上記に鑑み本発明は、センタが特別なアルゴリズム、すなわちセンタだけが秘密に保持するセンタアルゴリズムを作成し、センタは、ソフトウェア並びにユーザのそれぞれに固有で公開され且つ半定期的に用いられる各ソフトウェア並びにユーザの識別子にセンタアルゴリズムを施して各ソフトウェア並びにユーザに専用の秘密アルゴリズムを作成し、ユーザ及びソフトウェアに供給するという準備を行った後、ソフトウェア供給体とユーザとの間で、ソフトウェアの供給が生じた場合、ソフトウェア供給体は、ユーザの識別子を供給対象となるソフトウェアの秘密アルゴリズムに入力することによって、供給対象となるソフトウェアとユーザとの間で同一且つ固有の暗号鍵を作成し、この暗号鍵に基づいて直接的又は間接的に供給対象となるソフトウェアの一部又は全部を暗号化してユーザへ供給し、ユーザは、使用時、供給されたソフトウェアの識別子を自己の秘密アルゴリズムに入力することによって、供給されたソフトウェアとユーザとの間で同一且つ固有の暗号鍵を作成し暗号化ソフトウェアを直接的又は間接的に復号化する方式により、正当なユーザは、簡単な操作によりソ

フトウェアの使用ができるが、その他のユーザは、コピーはできても使用できないソフトウェアプロテクト方式を実現した。

## 本発明の概要

本発明は、センタ（管理機関）が設けられており、センタは、センタアルゴリズムを秘密に保持する。センタは、このセンタアルゴリズムとユーザ及びソフトウェアの識別子（名前、住所、管理番号、任意の符号、記号、数字等）から秘密アルゴリズムを作成し、ユーザ及びソフトウェアに配布する。尚、識別子は、公開、非公開、又は固有で公開され且つ半定期的に用いられるものであることが例示される。センタがソフトウェアに対して作成した秘密アルゴリズムを供給する相手となるソフトウェアとは、例えばソフトウェア自体、ソフトウェア供給体、あるいはその両者等である。ここでソフトウェアとは、例えばアプリケーションプログラム、OSプログラム、ユーティリティプログラム、その他のプログラムを示すものであり、センタで作成される秘密アルゴリズムは、このソフトウェアの内容を問わずユーザへの供給の対象となる1つ1つのそれぞれに配布されるものである。ソフトウェア供給体とは、ソフトウェアをユーザへ供給するものであって、例えばソフトハウス、関連メーカ、小売店、(Vender)、ソフトウェアを供給するソフトウェア、又は装置、その他有償、間接的に無償でユーザへ対象となるソフトウェアを供給する存在である。このソフトウェア供給体はセンタと合体する場合もあり、センタはユーザと合体する場合もある。尚、ソフトウェア供給体もソフトウェアを使用する立場になればユーザとなるのである。尚、ユーザ及びすくなくともターゲットとなったソフトウェアは、予めまたは、各動作の直前までにセンタから秘密アルゴリズム、識別子の供給を受けているものとする。ユーザとは、使用者の他、例えば使用者が直接又は間接に所有するソフトウェアを実行させる装置、その付属装置、あるいは、ソフトウェア自体、等が示される。本発明の動作概要は、図1に示す様なものとなる。ソフトウェア供給体からユーザに配布されるプログラム(P)の一部を、プログラム固有の第2暗号鍵(K)と暗号化アルゴリズムによりあらかじめ暗号化しておく(P')。ユーザは、プログラムをインストールする際に、自らの識別子(IDu)をソフトウェア供給体に申請する。ソフトウェア供給体では、申請された識別子(IDu)と、プログラム固有の秘密アルゴリズムを用いて第1暗号鍵を作成し、この第1暗号鍵と暗号化アルゴリズムを用いて先の第2暗号鍵Kを暗号化し(K')、この(K')をユーザに配布する。ユーザは、配布された暗号化第2暗号鍵(K')と、暗号化プログラム(P')に添付(あるいは別添)のインストールソフトを用いて暗号化プログラム(P')をインストールする。インストールソフトは、暗号化第2暗号鍵(K')を含んだローダを作成し、暗号化プログラム

(P')とリンクする。ローダは、実行する度にユーザの秘密アルゴリズムとプログラムの識別子を用いて共有鍵(第1暗号鍵)を作成し、復号アルゴリズムと共に暗号化第2暗号鍵(K')を復号化して第2暗号鍵を作成し、この第2暗号鍵と復号化アルゴリズムによって暗号化プログラム(P')を復号する(P)。尚、上記は、暗号鍵を2つ用いてプログラムに暗号化復号化を施すものであり、間接的方法であるが、このような複数の暗号鍵を使用する間接的方法に限らず1つの暗号鍵(自己の秘密アルゴリズムと相手の識別子とから得られる共有鍵)を使用してプログラムを暗号化復号化する直接的方法であってもよい。センタアルゴリズムの作成方法、秘密アルゴリズムの作成方法、及び共有する暗号鍵の作成方法、エンティティ、識別子の定義等、共有鍵を作成するまでの行程に係わる方法及び内容は、特開昭63年第36634号公報、特開昭63年第107667号公報に記載されている通りである。尚、識別子を秘密アルゴリズムに施す場合、上述の公報に記載されている方式の他、論文(松本、高嶋、今井 "簡易型一方向性アルゴリズムの構成" 信学技報IT89-23, July 1989)に記載された方式が好適に利用される。又、2つ以上の暗号化乃至復号化アルゴリズムは、同一であってもよい。これは例えば、DES(Data Encryption Standard)方式、FEAL(Fast Data Encipherment Algorithm)方式等が示されるが、速度、暗号の程度によっては、その他の方式が採用されてもよい。

#### 【0004】

【実施例】図2は、本発明の1実施例を説明するための図である。尚、センタについては上述したものであり説明は省略した。

#### 【条件】

①ユーザは、センタから秘密アルゴリズム及び本人認証アルゴリズムを記憶した担体(例えば、ICカード、ディスクその他の記憶媒体等)及びこの担体と共同して動作する担体実行装置及び識別子を所有する。ソフトウェア供給体も同様に、アルゴリズムを記憶した担体及び担体実行装置を所有している。尚、ソフトウェア供給体は、特に担体及び担体実行装置という構成でアルゴリズムを所有している必要はない。

②バックアップは自由に行なえる。

③全ソフトハウス(ソフトウェア供給体)、全プログラムについて汎用である。

#### 【環境及び定義】

ソフトハウス(ソフトウェア供給体)：販売するプログラム(P)に固有の秘密アルゴリズム(プログラム識別子をIDpとする)を管理する。販売する際は、プログラム(P)の一部を任意(ただしPに固有)の乱数(K)(第2暗号鍵)と暗号化アルゴリズムとを用いて暗号化したプログラム(P')を配布する。(P')は、実行できないファイルである。暗号化プログラム

(P')を購入したユーザが、自らの識別子(IDu)を申請するので、正規ユーザからの申請であれば識別子(IDu)と、秘密アルゴリズムを用いて第1暗号鍵を作成し、この第1暗号鍵と暗号化アルゴリズムを用いて第2暗号鍵である乱数(K)を暗号化して暗号化乱数(K')を作成し、ユーザに対して暗号化乱数(K')を配布する(K'には、第1暗号鍵作成システムに付随するデータを含む。)

ユーザ：購入したプログラムをインストールする際に、ソフトハウスに対して自らの識別子(IDu)を申請する。尚、申請しなくてもよい場合もある。ソフトハウスから送られてくるK'をインストールソフトに入力する。インストールソフトにより作成されたローダを用いてプログラムを使用する。

インストールソフト：ユーザにより入力された識別子(IDp)、暗号化乱数(K')を用いてローダを作成し、暗号化プログラム(P')とリンクする。このインストールソフトは、暗号化プログラム(P')に添付、又は別途購入(無料配布)され、すべてのプログラムに共通である。

ローダ：ユーザが所持する担体及び担体実行装置を用い、自らファイル中に所持するプログラムの識別子(IDp)、暗号化乱数(K')をパラメータとして与え、暗号化プログラム(P')を復号しプログラム(P)を得る。但し、Pはメモリ上のみ存在し、ファイル化はされない。また、P'は、必要とされる部分だけが復号され、完全な形としてのプログラム(P)は存在しない。また、ローダには復号ルーチンは存在しない。

担体実行装置：ターゲットプログラム実行装置(例えばパソコン、オフコン、WSその他の実行装置)と一体化、別体化、内蔵化して接続(赤外線、電気、光、超音波、電波等の様式で)された装置であって例えば、担体(例えばICカードディスクその他の記憶媒体)のリーダ、ライター機構を具備するものであり、内部に復号プログラム(復号アルゴリズム)(AdapterCipherEngine:ACE)を内蔵し、担体が出力する乱数(K)を基に、暗号化プログラム(P')を復号する。乱数(K)は、担体実行装置でのみ存在し、外部には出力されない。また、将来性を考え、ACEは、バージョンアップ又は、ACEそのものの変更(DES→FEAL等)を可能とするのが望ましい。尚、担体及び担体実行装置は、一例であって、その他これらを合体させターゲットプログラム実行装置に内蔵化、一体化、別体化させたものあるいは付属的に接続させたものあるいは、プログラム化し、ターゲットプログラム実行装置内部で動作させるもの等であってもよい。

#### 【0005】【方法】

「ソフトハウス側の処理～プログラムの配布前～」

・ソフトハウスは、ターゲットとするプログラム(P)を複数のロードブルモジュールに分割する。また、全モ

ジュールが、一度にメモリ上にロードされない様に、プログラムを設計する。

- ・分割したそれぞれのモジュールの、任意の一部を暗号化する。暗号部のアドレス情報は、暗号化プログラム(P')中に存在する。アドレス情報自体も暗号化されていても良い。

- ・暗号化に用いる乱数(第2暗号鍵)(K)は、プログラム毎にユニークである。更に、モジュール毎にユニークとしても良い。

- ・この暗号化の手段は、担体実行装置内蔵の復号プログラム(復号アルゴリズム)ACEで対応できる方法ならば、どのような方法でも構わない。ソフトウェア供給体が独自のACEを用意し、ユーザに配布するのであれば、全ソフトウェア供給体共通でなくとも良い。

「ユーザ側の処理～プログラム購入時～」

(担体、担体実行装置、インストールソフトは既に用意されているとする)

- ・ソフトウェア供給体に対して、ユーザ登録し、本人識別子を申請する。

「ソフトハウス側の処理～ユーザ登録時～」

- ・ユーザが申請した識別子(IDu)と、配布したプログラムに固有の秘密アルゴリズム(Xp)を用いて、乱数(K)を暗号化する(K')。尚、秘密アルゴリズム(Xp)を使用する際、図2では、パスワード符号(PIN-P)を入力し、本人認証アルゴリズム(CHA-P)によって本人と一致不一致を判断している。本人認証アルゴリズム(CHA-P)及びパスワード符号(PIN-P)は、センタから秘密アルゴリズム(Xp)が提供される際、一緒に添付されて来るものであるが、その使用は任意であり、又センタからの提供も任意である。ユーザ側の本人認証アルゴリズム(CHA-U)及びパスワード符号(PIN-u)も同様である。ソフトウェア供給体は、暗号化乱数(K')をユーザに送付する。送付の方法は、電話、ファックス、パソコン通信、又はフロッピー等どのような方法でも構わない(Pの暗号化にDESを用いた場合、ユーザに送付する情報量は、16バイト(文字列に変換して32文字)となる。)。また、プログラムの識別子(IDp)は、暗号化乱数(K')と共にユーザに通知しても良いが、暗号化プログラム(P')配布時に、パッケージに印刷する等の方法も可能である。「ユーザ側の処理～プログラムインストール時～」

- ・ユーザは、インストールソフトを起動し、送られてきた暗号化乱数(K')と、プログラム識別子(IDp)を入力する。

- ・インストールソフトは、入力された暗号化乱数(K')とプログラム識別子(IDp)を用いてローダを作成し、暗号化プログラム(P')とリンクする(ローダ付きP')。ローダとは、OS(MS-DOS等)が処理できるユーティリティであり、OSと、暗号化プログラム(P')の仲介をする。この時点では、まだ暗

号化プログラム(P')は暗号化されたままである。

「ユーザ側の処理～プログラム実行時～」

- ・ローダ付きP'を起動し、担体の本人認証を行なう。
- ・ローダは、プログラム識別子(IDp)と秘密アルゴリズム(Xu)から第1暗号鍵(Kup)を作成し、暗号化乱数(K')を担体実行装置に与え、第1暗号鍵(Kup)と復号プログラム(D)により、暗号化乱数(K')を復号させる。但し、復号した乱数(K)は、担体実行装置の中にとどまり、外部には出力されない。
- ・ローダは、担体実行装置に暗号化プログラム(P')の暗号部分を与え、復号プログラム(DE)と乱数(K)によって復号させ、プログラムPを得て実行させる。

- ・ローダは常にプログラム(P)の実行状態を監視し、暗号化プログラム(P')の暗号部分が読み込まれる度に、担体実行装置に復号させる。尚、暗号化プログラム(P')は、それ自体では解読不可能であることからさまざまな態様で正当なユーザのみに配送可能となる。これは例えば、

- ・CD-ROM等の高容量記録媒体中に秘密アルゴリズムを既にまたは予約した状態で付帯する複数のプログラム(但し、パスワードを与えないと機能が制限されている)を収録し、秘密アルゴリズムを既にまたは予約した状態で付帯するユーザは試用の後、気に入ったプログラムのパスワード、識別子、を使用料を払って取得する態様。等である。尚、ソフトウェア供給体にとっても以下のような利便性がある。

- ・ソフトウェア供給体は、暗号化したプログラムをプレスすれば良いので、量産できる。

- ・必要とするハードウェアは、複数のソフトウェア供給体で利用できる。

【0006】更に他の実施例を図3に示す。図3は、図2で示した実施例においてさらに第3の暗号鍵及び暗号アルゴリズム、復号アルゴリズムを加えたものである。第1の暗号鍵(Kup)は、秘密アルゴリズムと相手(ユーザからすればターゲットプログラム)の識別子(IDp)を施して算術的に得られる。ソフトウェア供給体においては、(Kpu)で示されている。第2の暗号鍵(r)は、乱数等の任意に設定されたものである。第3の暗号鍵(K2)も第2暗号鍵と同様任意に設定されたものである。ソフトウェア供給体は、プログラム(P)の一部乃至全部を、第3暗号鍵(K2)と暗号アルゴリズム(E3)とにより暗号プログラム(P')に変換する。更に、ソフトウェア供給体は、第3暗号鍵(K2)の一部乃至全部を、第2暗号鍵(r)と暗号アルゴリズム(E2)とにより暗号化第3暗号鍵(K2')に変換する。更に、ソフトウェア供給体は、第2暗号鍵(r)の一部乃至全部を、第1暗号鍵(Kpu)と暗号アルゴリズム(E1)とにより暗号化第2暗号鍵(E(r))に変換する。ソフトウェア供給体は、暗号

プログラム ( $P'$ )、暗号化第2暗号鍵 ( $E(r)$ )、暗号化第3暗号鍵 ( $K2'$ ) をユーザに供給する。ユーザは、暗号化第2暗号鍵 ( $E(r)$ ) を第1暗号鍵 ( $Kup$ ) と復号アルゴリズム ( $D1$ ) とにより、復号化した第2暗号鍵 ( $r$ ) を作成し、この第2暗号鍵 ( $r$ ) と復号アルゴリズム ( $D2$ ) とにより暗号化第3暗号鍵 ( $K2'$ ) を復号化して第3暗号鍵 ( $K2$ ) を作成する。この第3暗号鍵 ( $K2$ ) と復号アルゴリズム ( $D3$ ) とにより暗号化プログラム ( $P'$ ) を復号化してプログラム ( $P$ ) 作成する。以上が図3の概略的動作を説明したものであるが、その他の動作は、図2の説明の通りである。

【0007】

【発明の効果】以上詳述した通り本発明は、センタという機関を通じてソフトウェア並びにユーザは固有の秘密アルゴリズムと識別子を付与されているという環境にお

いて、ユーザは、暗号化されたソフトウェアを所持し、必要なときだけ自分の秘密アルゴリズムにソフトウェアの識別子を入力するだけで、これを簡単に復号使用することから、操作が簡単で、しかも、ユーザは、秘密アルゴリズムを所有してさえいれば、あとは、ソフトウェアが追加、変更されようと、識別子が入手できる限りそのソフトウェアが使用出来ることとなり、ユーザの負担は、小さくなる。これに対し、その他のユーザにとっては、暗号化されたソフトウェアを入手してもその解読は、ほぼ不可能であることから、充分なプロテクトがなされるものである。

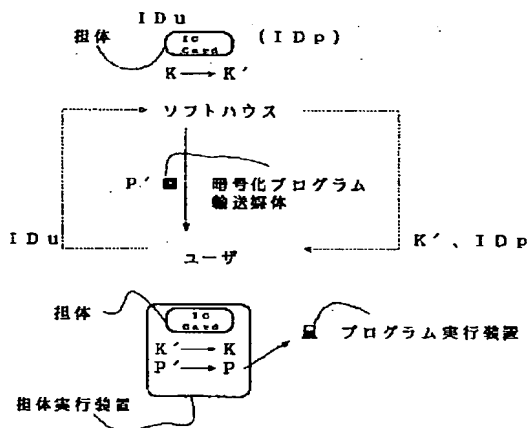
【図面の簡単な説明】

【図1】

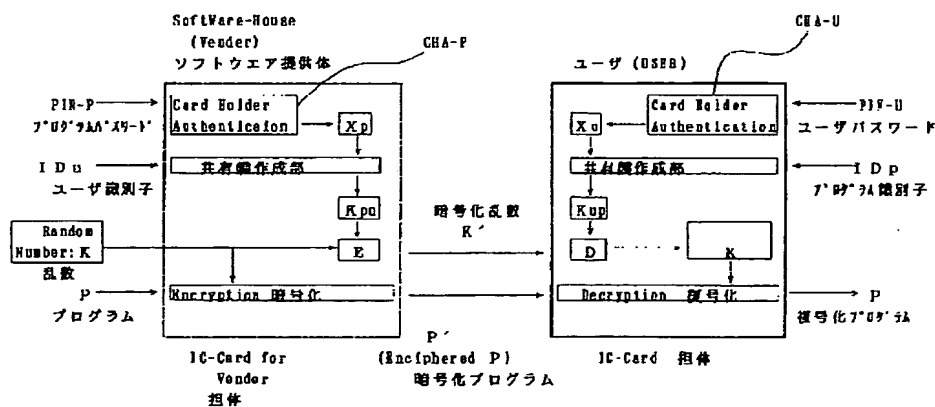
【図2】

【図3】本発明を説明するための図である。

【図1】



【図2】



【図3】

